WEST Search History

Hide Items Restore Clear Cancel

DATE: Monday, January 23, 2006

Hide?	Set Name	Query	Hit Count
		DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=ADJ	
□	L10	L8 and (home network)	2
□	L9	L8 and (visited network)	0
□	L8	L7 and ((subsriber or user) adj2 profile)	30
□	L7	L6 and @AD<20000530	91
□	L6	L5 and l4	91
□	L5	database near8 (access control)	1813
□	L4	L1 and @AD<20000530	1354
□	L3	L2 and @AD<20000530	5
□	L2	(store or storing or database) near8 (access near4 (mode or profile or authorized)) near8 ((contol or controlling) adj3 access)	21
□	L1	(store or storing or database) near8 (access near4 (mode or profile or authorized))	3947

END OF SEARCH HISTORY

Previous Doc Next Doc Go to Doc#
First Hit Fwd Refs

□ Generate Collection

L8: Entry 2 of 30 File: USPT Aug 16, 2005

DOCUMENT-IDENTIFIER: US 6931402 B1
TITLE: Profiling system for controlling access for a plurality of users to a plurality of objects located in at least one electronic database

Application Filing Date (1):
20000228

Brief Summary Text (5):
Profiling systems have been developed to control access to objects located in electronic databases. The profiling systems commonly create and maintain profiles of users who are entitled to some level of access to objects in the electronic databases controlled by the system. The access to the object may be read-only or viewing access, limited modify or write access, or full access to read and write (view or modify) access to one or more objects in the databases.

Brief Summary Text (6):
Each profiling system generally includes a profile database, the profile database having a number of access records. Each access record may detail user access rights to objects located in databases whose access thereto is controlled by the profiling system. Accordingly, a profiling system may be employed to control one or more databases located on a single computer, network of computers, or network of network of computers (commonly called the Internet). For example, many companies have established Intranets, which are private, controlled access databases accessible via the Internet. In this case, an Intranet profiling system may include a record with a fixed number of attributes (or fields) for each employee or user entitled to access objects within the databases of the Intranet.

Brief Summary Text (9):
With the advent of Extranets, the number of records required per user in the profile system may increase further. In order to provide an Extranet user access to an object located in a foreign Intranet, the Intranet profiling system would need to include security data that gives the user access to the needed object. For example, an employee of Company A may require access to an object located in a database of the Intranet of Company B (such as legitimate access to a report) where an Extranet is formed between the Intranet of Company A and B. Presently, the profiling system for the Intranet of Company B would need to include security data for the employee of Company A that enables the employee to have access to the object (such as a report) located in a database of the Intranet of Company B. This may cause replication of user information across several profiling systems. Consequently, a need exists for a profiling system that enables users to obtain access to different objects or different forms of access to objects in databases while not requiring duplicate information to be stored within a database of the profiling system.

Detailed Description Text (10):
As noted above, FIGS. 1-3 are diagrams of exemplary database structures for a profiling system and method in accordance with the present invention. FIG. 1 is diagram of an exemplary vertical component database. FIG. 2 is a diagram of an exemplary horizontal component or access Matrix database and FIG. 3 is a diagram of

Previous Doc Next Doc Go to Doc#
First Hit Fwd Refs

□ Generate Collection

L8: Entry 9 of 30 File: USPT Dec 31, 2002

DOCUMENT-IDENTIFIER: US 6502193 B1
TITLE: Software access

Application Filing Date (1):
19990330

Brief Summary Text (5):
In a distributed environment, the application or database may be installed on a site remote to the user, across one or more networks. To run the application or access the database, the user needs routing (or "connect") information of some sort, such as a network address. If the user wants to access a database directly, they need connect information for the database. If the user wants to run an application and the application is simply a front end to a database, the connect information the user needs is effectively, again, connect information for the database itself. Where the user can get connect information to a database, there is a potential weakness in access control.

Brief Summary Text (6):
Access control arises where there is a requirement for access restrictions to an application or database, for instance such that it can be used by subscribers only. Alternatively, it may be that some users can use all the functionality available while other users are barred from some functionality, for instance because of rank or job description. This situation would arise where account staff need both read and write access to a company's accounts databases but staff elsewhere in the company might be limited to read access only, and to accessing data relating only to themselves.

Brief Summary Text (8):
In order to provide a security check, it is known to write an authentication process into an application, or database front end, so that it will only run when a valid identity code (ID) and a password have been entered by the user. The application or front end may also have for instance a stored set of "user profiles" which allow it to tailor the capabilities it offers to a user to a limited set of capabilities for which the user is specifically registered.

Brief Summary Text (23):
It is known for a user to have a user profile for a database or software process. The user profile is allocated to the user and holds access information (defines the access rights) for that user in respect of a database or software process. User profiles might be stored with the database or software process and the user identification data, which the individual user knew and entered, is used by the database or software process to select and apply the relevant user profile. This suffers from the problem that there has to be a profile for every user. This can take up significant storage space.

Brief Summary Text (24):
In embodiments of the present invention, the access information store holds identifiers for data sets, or selections of functionality. It does not hold user profiles. When a user first enters an ID and password, the substitute login means

Previous Doc Next Doc Go to Doc#
First Hit Fwd Refs

□ Generate Collection

L8: Entry 5 of 30 File: USPT Feb 24, 2004

DOCUMENT-IDENTIFIER: US 6697806 B1
TITLE: Access network authorization

Application Filing Date (1):
20000519

Brief Summary Text (20):
In one aspect of the inventions for user access profile inheritance, the database system receives an update request from the access server to update a user access profile through inheritance. The database system then processes the update request to inherit user profile information from a user profile data structure. The database system updates the user access profile with the user profile information.

Brief Summary Text (23):
In another aspect of the inventions for user access profile mobility, the database system receives user information. The database system then processes the user information to determine if a user access profile is local within a local database system. The database system generates and transmits a request to retrieve a user access profile from a second database system external to the local database system in response to the determination that the user access profile is not local.

Brief Summary Text (38):
In another aspect of the inventions for switching access by a user, switching access by a service provider, and dynamic access control, the database system receives a request. The database system processes the request to determine if the switching of the access is allowed. The database system then generates an instruction to switch access in response to the determination that the switching is allowed.

Drawing Description Text (9):
FIG. 7 illustrates a table for a user access profile in an example of the invention.

Drawing Description Text (10):
FIG. 8 illustrates a flowchart for an access server for inheriting a user access profile in an example of the invention.

Drawing Description Text (11):
FIG. 9 illustrates a flowchart for a database system for inheriting a user access profile in an example of the invention.

Drawing Description Text (15):
FIG. 13 illustrates a flowchart of user access profile mobility in an example of the invention.

Detailed Description Text (5):
The access network 520 provides an interface between the user network 510 and 560 and the service networks 530 and 540. The interface function provides user access profiles, security, switching, and caching. The user network 510 and 560 could be a